

Wisconsin Legislative Council

Wisconsin Legislator Briefing Book 2007-08

N-1 **Major Privacy
Laws in
Wisconsin**

N-8 **Frequently
Asked
Questions**

N-9 **Glossary of
Terms and
Abbreviations**

N-10 **Additional
References**

By:
Dan Schmidt
Senior Analyst

Chapter N

Privacy

There is no particular state agency with general responsibility for privacy in Wisconsin. Instead, the state relies on a number of privacy laws that are generally enforced privately in the case of civil violations or by local district attorneys in the case of criminal violations.

The primary privacy law enacted in 2005-06 was 2005 Wisconsin Act 138. 2005 Act 138 generally requires Wisconsin businesses to notify individuals of unauthorized acquisition of their personal information in the care or custody of the business.

Privacy issues that may recur in the 2007-08 Session include: privacy of professional sports locker rooms; crime victim privacy; possession of nude pictorials without the subject's consent; identity theft; and limiting the use of individuals' Social Security numbers as identifying information.

Major Privacy Laws in Wisconsin

The laws described in the following paragraphs were selected as a representation of the major privacy provisions in Wisconsin. This is not an exhaustive list of the privacy provisions included in the Wisconsin statutes. It represents a listing of some of the more significant privacy provisions that are often the subject of constituent questions.

Wisconsin statutes recognize an individual's right to privacy.¹ An invasion of privacy is defined as any of the following:

- An intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner that is actionable for trespass.
- The use, for advertising purposes or for purposes of trade, of the name, portrait, or picture of any living person, without hav-

ing first obtained the written consent of the person or, if the person is a minor, of his or her parent or guardian.

- Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed.
- Conduct involving a representation that depicts nudity without the knowledge and consent of the person who is depicted nude in a circumstance in which the person has a reasonable expectation of privacy, regardless of whether there has been a criminal action related to the conduct or regardless of the outcome of such a criminal action.

However, it is not an invasion of privacy to communicate any information available to the public as a matter of public record.

Under Wisconsin law, a person whose privacy has been invaded is entitled to the following remedies:

- Equitable relief to prevent and restrain an invasion of privacy, excluding prior restraint of constitutionally protected speech;
- Compensatory damages based on the plaintiff's loss or the defendant's unjust enrichment, if proven; and
- Reasonable attorney fees.

If the court determines that an action for invasion of privacy is frivolous, the court must award the defendant reasonable fees and costs relating to the defendant. A frivolous action is an action that was commenced in bad faith or for harassment purposes or an action that was commenced without an arguable basis.

Crime of Invasion of Privacy

Wisconsin law specifically prohibits an individual from engaging in any of the following crimes of invasion of privacy:²

- Installing or using a surveillance device in a private place with the intent to observe a nude or partially nude person without the consent of the person observed.
- Looking into, for the purpose of sexual arousal or gratification, a private place that is or is part of a public accommodation (public restrooms, etc.) in which a person may be nude or partially nude, regardless of whether an individual is present or not.
- Enters another person's private property without consent and views an individual who has a reasonable expectation of privacy in that part of the dwelling, without consent, for the purposes of sexual gratification or arousal and with the intent to intrude upon or interfere with the individual's privacy.

If a person is convicted of an invasion of privacy crime, he or she is guilty of a Class A misdemeanor and may be fined up to \$10,000 or imprisoned for nine months or both. The court may also order an individual convicted, adjudicated delinquent, or found not guilty by reason of mental disease or defect to register with the Department of Corrections as a sex offender.

Representations Depicting Nudity

In addition to the aforementioned crimes of invasion of privacy, Wisconsin law prohibits certain representations depicting nudity without the express permission of the subject of the depiction.³ A representation is defined as a photograph, exposed film, motion picture, videotape, other visual representation, or data that represents a

visual image. Specifically, the law provides that anyone who engages in the following may be found guilty of a Class I felony:

- a. Captures a representation that depicts nudity without the knowledge and consent of the person who is depicted nude while that person is nude in a circumstance in which he or she has a reasonable expectation of privacy, if the person knows or has reason to know that the person who is depicted nude does not know of and consent to the capture of the representation.
- b. Makes a reproduction of a representation that the person knows or has reason to know was captured in violation of par. a. and that depicts the nudity depicted in the representation captured in violation of par. a., if the person depicted nude in the reproduction did not consent to the making of the reproduction.
- c. Possesses, distributes, or exhibits a representation that was captured in violation of par. a. or a reproduction made in violation of par. b., if the person knows or has reason to know that the representation was captured in violation of par. a. or the reproduction was made in violation of par. b., and if the person who is depicted nude in the representation or reproduction did not consent to the possession, distribution, or exhibition.

Class I felony convictions under this provision are punishable by a fine of up to \$10,000 or imprisonment up to three years and six months, or both.

Identity Theft

The unauthorized use of personal identifying information, or identity theft,⁴ is prohibited in Wisconsin. A person who intentionally uses or attempts to use personal identifying information or personal identification documents (a birth certificate, PIN number, or financial transaction card) of another individual to obtain credit, money, goods, services, or anything of value, without that individual's authorization or consent, to avoid civil or criminal process or penalty, or to harm the reputation, property, person, or estate of an individual, is guilty of a Class H felony. A Class H felony is punishable by imprisonment for up to six years, a fine of up to \$10,000, or both.

For the purposes of this statute, personal identifying information includes an individual's:

- Name.
- Address.
- Telephone number.
- Driver's license number.
- Social Security number.
- Employer or place of employment.
- Employee identification number.
- Mother's maiden name.
- Financial account numbers.
- Taxpayer identification number.
- Deoxyribonucleic acid (DNA) profile.
- Any number or code that can be used alone or with an access device to obtain money, goods, services, or any other thing of value.

- Unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
- Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.
- Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

In addition, the law provides that if any individual reports an identity theft violation to the law enforcement agency where the individual resides, but the violation occurs outside of that law enforcement agency's jurisdiction, the law enforcement agency receiving the complaint must prepare a report on the violation and forward it to the law enforcement agency in the appropriate jurisdiction.

Disposal of Records Containing Personal Information

Wisconsin law prohibits financial institutions, medical businesses, and tax preparation businesses in this state from disposing of records that contain personal information unless the personal information is first rendered undiscoverable.⁵ The statutes provide that these businesses may discard the records only after they have done one of the following prior to disposal:

- Shred the records;
- Erase the personal information contained in the records;
- Modify the records to make the personal information unreadable; or
- Take actions that the businesses reasonably believe will ensure that no unauthorized individual will have access to the personal information contained in the records prior to their destruction (e.g., locked dumpsters).

For the purposes of this statute, personal information generally includes medical information, account or credit information, account or credit application information, and tax information, by which an individual is capable of being associated through one or more identifiers.

A business that improperly disposes of such records may be required to forfeit up to \$1,000 per violation and may be held liable for damages received by the individual whose personal information was disposed of improperly. A person who uses personal information that was improperly disposed of is also liable for damages and may be fined \$1,000, imprisoned for 90 days, or both. Such a violation is commonly referred to as "**dumpster diving**."

Notice of Unauthorized Acquisition of Personal Information

2005 Wisconsin Act 138 requires certain business entities to notify individuals of unauthorized acquisitions of personal information.⁶ If an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of the personal information.

General Issues. The law applies to entities that: (a) conduct business in Wisconsin and maintain personal information in the course of business; (b) license personal information in Wisconsin; (c) maintain for a Wisconsin resident a depository account; or (d) lend money to a resident of Wisconsin. An "entity" also includes: (a) the state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by

the constitution or any law, including the Legislature and the courts; and (b) a city, village, town, or county.

“Personal information” means an individual's last name and the individual's first name or first initial, **in combination with and linked to** any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (d) the individual's DNA profile; and (e) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical characteristic.

If an entity whose principal place of business is **not** located in Wisconsin knows that personal information pertaining to a Wisconsin resident has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each Wisconsin resident who is the subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident.

If a person, other than an individual, that stores personal information pertaining to a Wisconsin resident, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the information must notify the person that owns or licenses the information of the acquisition as soon as practicable.

If, as a result of a single incident, an entity is required to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity must, without unreasonable delay, notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the individuals.

An entity is **not** required to provide notice if: (a) the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information; or (b) the personal information was acquired in good faith by an employee or agent of the entity and the personal information is used for a lawful purpose.

Timing and Method of Notice. An entity must provide the required notice within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination of reasonableness must include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. Notice must be provided by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject, and if the entity has not previously communicated with the subject, the entity must provide notice by a method reasonably calculated to provide actual notice to the subject. Upon written request by a person who has received a notice under the Act, the entity that provided the notice must identify the personal information that was acquired.

Exemptions. These notice provisions do not apply to financial institutions that are subject to and in compliance with federal law relating to disclosure of nonpublic personal information or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. In addition, the provisions do not apply to health plans, health care clearinghouses, or health care providers, if the entity complies with federal law relating to security and privacy of information maintained by those entities.

In addition, a law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under the Act for a period of time. The notification process must begin at the end of that time period. If an entity receives such a request, it may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

Privacy of Health Care Records

Wisconsin law requires that all patient health care records remain confidential unless a patient or a person authorized by the patient gives explicit **informed consent** to the release of the patient's health care record or unless the situation comes within one of the exceptions listed in the law.⁷ A patient health care record is defined as any record related to the health of a patient prepared by or under the supervision of a health care provider. Informed consent to disclose patient health care records to an individual, agency, or organization must be written. A statement of informed consent must include all of the following:

- The name of the patient whose record is being disclosed;
- The type of information to be disclosed;
- The types of health care providers making the disclosure;
- The purpose of the disclosure;
- The individual, agency, or organization to which disclosure may be made;
- The signature of the patient or the person authorized by the patient and, if signed by a person authorized by the patient, the relationship of that person to the patient or the authority of the person;
- The date on which the consent is signed; and
- The time period during which the consent is effective.

Under certain specified circumstances, patient health care records may be released without the informed consent of the patient. Included in the list of exceptions are release of information to other health care workers who are caring for the patient, government agencies with certain health care responsibilities, and certain health care research organizations. Generally, recipients of patient health care information without informed consent must keep that information confidential and may not disclose such information further. Although similar to general patient health care records, the treatment of mental health records and human immunodeficiency virus (HIV) test results is governed by separate statutes. Mental health record access laws are in s. 51.30 (4), Stats., and HIV test result laws are in s. 252.15, Stats.

Violations of the laws on confidentiality of patient health care records are punishable by penalties, with the severity of the penalty varying depending on whether the violation was negligent, intentional, or intentional with a pecuniary gain. Private lawsuits are also authorized in which a plaintiff may recover actual damages, specified exemplary damages, and costs and attorney fees.

Prohibition on Wiretapping

Wisconsin law generally prohibits the intentional actual or attempted interception, actual or attempted use of a device to intercept, intentional alteration, and actual or attempted disclosure of information obtained through the interception of wire, electronic, or oral communication.⁸ Generally, a person not acting under color of law may intercept wire, electronic, or oral communication, commonly referred to as wiretapping, only if that person is a party to the communication or has prior consent from one of the parties to the communication. A person is strictly prohibited however from performing any interception with the purpose of violating a law or committing any other injurious act. Violations of the wiretapping prohibitions are punishable by a fine of up to \$10,000, imprisonment for up to seven years and six months, or both.

Prohibition on Unauthorized Telephone Solicitations

Residents of Wisconsin who do not wish to receive telephone solicitations may request to be included on the state's telephone nonsolicitation directory.⁹ The directory, also referred to as the **Do-Not-Call List**, is maintained by the Department of Agriculture, Trade and Consumer Protection (DATCP). There is no charge to the resident for this service. Companies engaging in telephone solicitation in Wisconsin must pay a registration fee that is proportional to the number of telephone lines used for solicitation. These fees are used to fund costs associated with the operation of the nonsolicitation directory.

A telephone solicitor or employee or contractor of a telephone solicitor may not make a telephone solicitation to a residential customer if that individual is listed in the nonsolicitation directory. A telephone solicitor also may not make a telephone solicitation to a nonresidential customer if the nonresidential customer (e.g., a business) has provided the solicitor with notice by mail that the nonresidential customer does not wish to receive telephone solicitations. Finally, a telephone solicitor may not require an employee or contractor to make a telephone solicitation in violation of the provisions of the nonsolicitation prohibition. These prohibitions do not apply if a telephone solicitation is made in response to the recipient's request for such a solicitation or when the recipient is a current client of the person selling property, goods, or services through telephone solicitation. The nonsolicitation prohibition does not apply to a nonprofit corporation, or its employees or contractors, that engages in telephone solicitation.

In addition, a telephone solicitor may not use a prerecorded message in a telephone solicitation without the consent of the recipient of the solicitation.

A person who violates the telephone solicitation regulations may be required to forfeit \$100 per violation. The DATCP enforces these provisions.

Collection of Social Security Numbers

General Issues. Federal law places a number of restrictions on state and local governmental use of an individual's Social Security number. For example, the Federal Privacy Act of 1974 generally prohibits federal, state, or local government agencies from denying to an individual any right, benefit, or privilege provided by law because that individual refuses to disclose his or her Social Security number. This prohibition does not apply if the disclosure is required by federal law or the disclosure is required by a federal, state, or local agency: (1) maintaining a system of records in existence and operating before January 1, 1975; and (2) if the disclosure was required under statute or regulation adopted prior to that date to verify the identity of an individual.

Federal law also authorizes several specific uses that a state or local government, or an agency thereof, may make of a person's Social Security number. For example, the Social Security Act authorizes states or local units of government to require persons to disclose their Social Security numbers and to utilize such numbers as a form of identification in the administration of a tax program, a general public assis-

tance program, a driver's license or motor vehicle registration program, or a blood donor program, and in the administration of laws relating to birth certificates.

While a state or local governmental agency is limited in its ability to require persons to disclose their Social Security numbers, those agencies are not prohibited from requesting that a person provide their Social Security number. However, if a state or local governmental agency requests a person to disclose his or her Social Security number under any situation, the Privacy Act of 1974 requires the state or local government agency to advise the individual whether the disclosure is mandatory or voluntary, under what statutory authority or other authority the Social Security number is requested, and what uses will be made of the Social Security number.

Recent Federal Laws. The federal Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) and the Balanced Budget Act of 1997 established a requirement that all states collect Social Security numbers as a condition of receiving federal funding for child support and family assistance programs. These laws were created to assist states and the federal government in finding and reducing the number of individuals evading child support payments. Thus, as a condition to receive any license in Wisconsin, an individual's Social Security number must be recorded on the license application. Social Security numbers are also required for records relating to a divorce decree, support order, paternity determination, and on death certificates.

Private Collection of Social Security Numbers. While the Social Security number is commonly used as a financial identifier, the federal government does not regulate the collection of Social Security numbers by private individuals or corporations. Certain industries (credit, banking, etc.) may require a Social Security number as a condition of conducting business; however, it is up to the discretion of the individual to decide to release or withhold a Social Security number in private matters.

Frequently Asked Questions

Q: Can I see my own medical records?

A: Yes. A health care provider must allow you to inspect your medical records during regular business hours if you provide reasonable notice of your intent to inspect the records. You may also receive a copy of your health care records; however, the health care provider may charge reasonable costs for providing copies.

Q: What must I do to get a copy of my medical records transferred from my health care provider to another health care provider, other organization, or individual?

A: You must provide the health care provider who is the custodian of the record with a **statement of informed consent**. The statement must include information specified in the statutes (described above under *Privacy of Health Care Records*).

Q: Can a private company require me to provide my Social Security number as a condition of engaging in business?

A: Yes. Federal law does not prohibit private business use of Social Security numbers for any legitimate purpose. Financial institutions and other creditors often use Social Security numbers as financial identifiers when checking credit histories.

You may refuse to provide your Social Security number on such occasions; however, the business making the request is under no obligation to provide goods or services if you refuse.

Glossary of Terms and Abbreviations

CIO – Chief Information Officer.

Do-Not-Call List – State's telephone nonsolicitation directory maintained by the DATCP.

PRWORA – Personal Responsibility and Work Opportunity Reconciliation Act.

UETA – Uniform Electronic Transactions Act.

Q: How can I prevent individual telemarketers from calling me in the future?

A: Federal law prohibits a telemarketer from calling again in the future if you ask the telemarketer not to call you again. If calls continue, you should monitor the frequency of calls and report them to the Federal Communications Commission (FCC).

Q: Can telemarketers call at any hour of the day or night?

A: Telemarketing call times are restricted to those hours between 8:00 a.m. and 9:00 p.m. Violations may be reported to the FCC.

Q: Are prerecorded telephone solicitations legal?

A: Only when you have given consent to a live caller to receive those messages. Violations may be reported to the Consumer Protection Division of the DATCP.

State Do-Not-Call List

1-866-966-2255
(1-866-9NO-CALL)

<https://nocall.wisconsin.gov/web/registration.asp>

Q: Who do I contact to put my name on the state nonsolicitation directory or Do-Not-Call list?

A: Contact the Consumer Protection Division of the DATCP at 1-866-966-2255 (1-866-9NO-CALL) or at <https://nocall.wisconsin.gov/web/registration.asp>.

Q: Is there a law that prohibits a person from sending me an unauthorized facsimile solicitation?

A: Yes. Wisconsin law prohibits a person from sending a facsimile solicitation unless **both** of the following apply:

- The document transmitted by facsimile machine does not exceed one page in length and is received by the person solicited after 9:00 p.m. and before 6:00 a.m.
- The person making the facsimile solicitation has had a previous business relationship with the person solicited.

A person may not send a facsimile solicitation to an individual who has stated, through facsimile transmission or written means, that he or she does not wish to receive those solicitations.

Q: Can my financial institution give or sell my personal information to interested parties?

A: Generally, no. The Federal Gramm-Leach-Bliley Act prohibits banks from sharing information with non-affiliated third parties unless **all** of the following occur:

- The financial institution clearly and conspicuously discloses to the consumer in writing, electronic, or other authorized format that such information may be disclosed to a third party.
- The consumer is given an opportunity, before the time that the information is initially disclosed, to direct the institution that such information not be disclosed to a third party.
- The consumer is given an explanation of how the consumer can exercise this nondisclosure option.

Q: I think telemarketers are getting my contact information from the state driver's license database. How can I prevent this?

A: You can designate that the Department of Transportation (DOT) not release your personal information in response to requests for the records of 10 or more drivers. This removes your name from the complete drivers' list that may be used as a telemarketing tool. The form is available from the Division of Motor Vehicles in the DOT.

Additional References

1. **National Conference of State Legislatures** (NCSL) Communications and Information Policy Committee Web site at <http://www.ncsl.org/programs/lis/cip/ciphome.htm>. NCSL publications that are not available on the NCSL Web site are usually available at no charge to legislators and staff. To order copies, contact the NCSL Publication Department at 303-364-7812.
2. **Federal Communications Commission** Web site at <http://www.fcc.gov/>.
3. **Office of Privacy Protection** at the DATCP Web site at <http://www.privacy.wi.gov/>.
4. The **Federal Trade Commission's** Web site on identity theft at <http://www.consumer.gov/idtheft/>.

¹ s. 995.50, Wis. Stats.
² s. 942.08, Wis. Stats.
³ s. 942.09, Wis. Stats.
⁴ s. 943.201, Wis. Stats.
⁵ s. 134.97, Wis. Stats.
⁶ s. 895.507, Wis. Stats.
⁷ s. 146.82, Wis. Stats.
⁸ s. 968.31, Wis. Stats.
⁹ s. 100.52, Wis. Stats.

Wisconsin Legislative Council

One East Main Street
 Suite 401
 Madison, WI 53703-3382

Phone: (608) 266-1304
 Fax: (608) 266-3830

www.legis.state.wi.us/lc